The Honorable Tana Lin

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

ANN MAYHALL, on behalf of her Minor Child, D.M., individually and on behalf of all others similarly situated,

Plaintiff,

V.

AMAZON WEB SERVICES, INC. and AMAZON.COM, INC.,

Defendant.

NO. 2:21-cv-01473-TL

PLAINTIFF'S OPPOSITION TO DEFENDANTS' MOTION TO DISMISS COMPLAINT

NOTING DATE: MARCH 11, 2022

ORAL ARGUMENT REQUESTED

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

TABLE OF CONTENTS

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

TABLE OF AUTHORITIES

Page(s)

Cases

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Statutes

Other Authorities

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

INTRODUCTION

This case arises out of the creation, dissemination, and storage of biometric data by Defendants Amazon Web Services, Inc. ("AWS") and Amazon.com, Inc. ("Amazon"). D.M., a minor, created a customized player in the NBA 2K video game. To do this, he took multiple pictures of his face with his cell phone and uploaded them via the NBA 2K app. He then logged on to his X-Box One in Illinois to create the custom player. When he clicked the button to create the player, he watched a circle on the screen go from 0% to 100%. Behind the scenes, and unbeknownst to D.M., AWS and Amazon were working to create, deliver, and store D.M.'s biometric data associated with his custom player—including D.M.'s face geometry.

Illinois' Biometric Information Privacy Act, 740 ILCS 14/1 ("BIPA") "regulat[es] the collection, use, safeguarding, handling, storage, retention, and destruction" of biometric data. *Id.* § 5(g). It governs private entities that possess, collect, capture, purchase, receive through trade, or otherwise obtain biometric data. *Id.* § 15. Defendants obtained and possessed D.M.'s biometric data but did not comply with BIPA's requirements.

Defendants seek to dismiss the Complaint by relying on factual assertions, mischaracterizations of Plaintiff's allegations, and inapposite cases. They argue they never possessed or obtained the biometric data because they "never interacted with D.M.," and never "controlled the data at issue." Defs.' Mot. Dismiss ("Def. Mot.") at 1. Plaintiff's actual allegations, however—examined in light of the relevant case law that Defendants ignore, and BIPA's plain language—plausibly allege that Defendants obtained and were in possession of the biometric data they created, disseminated, and stored in their servers.

Despite being in possession of biometric data, Defendants failed to develop, publish, and comply with a written retention and destruction policy as required by BIPA § 15(a). Defendants also failed to inform D.M., or his authorized representative, that they were collecting or storing D.M.'s biometric data; failed to inform him of the specific purpose and length of term for that collection, storage, and use; and failed to first obtain a written release as required by § 15(b). Moreover, Defendants violated § 15(c) when they received money to create, disseminate, store,

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

and share access to biometric data. They violated § 15(d) when they disseminated and/or disclosed the biometric data to multiple locations, to, through, or among others, without Plaintiff's knowledge or consent. Further, Defendants profited off of the biometric data of Plaintiff and the Class, while "exposing [them] to a heightened risk of privacy and informational harms and depriving them of their control over their biometric data," (Compl. ¶ 241), and such allegations "sufficiently state[] a claim for unjust enrichment under Illinois law." *Vance v. Amazon.com, Inc.*, 525 F. Supp. 3d 1301, 1328 (W.D. Wash. 2021).

Finally, Plaintiff alleges the interconnection between AWS and Amazon, including their "shared facilities" and a "shared infrastructure," through which they create, disseminate, and store the biometric data at issue. Plaintiff also identifies specific causes of action against each Defendant. Thus, Plaintiff complies with Rule 8(a)'s notice pleadings standard as Amazon is properly on notice of the claims against it. *See* Counts V-IX.

Accordingly, Defendants' Motion to Dismiss should be denied.

FACTUAL BACKGROUND

NBA 2K is a basketball video game published each year by Take 2 Interactive Software, Inc. and/or its wholly-owned subsidiary 2K Games, Inc. (collectively "Take 2"). Compl. ¶ 9. For the NBA 2K games, Take 2 utilizes cloud-computing services of AWS and Amazon. *Id.* ¶ 10. Cloud-computing is the on-demand delivery of technology services over the internet and includes, among other things, computing power, storage, networks, machine learning, analytics, and related infrastructure. *Id.* ¶¶ 39-58. Take 2 also utilizes Amazon CloudFront, which is a content storage and delivery network that "speeds up" content delivery by distributing and storing content at various "regional" and "edge" data center locations. *Id.* ¶¶ 47-58, 107.

AWS and Amazon have "shared facilities" and a "shared infrastructure," including data centers, CloudFront IP addresses, servers, networks, and other equipment utilized by AWS that Amazon owns and operates. *Id.* ¶¶ 59-63. Thus, while AWS enters contractual relationships with video game companies such as Take 2 (*id.* ¶¶ 65, 67-68), AWS utilizes Amazon's "shared facilities" and "shared infrastructure" to provide such services (*id.* ¶¶ 66, 61-63, 9, 11).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Take 2 also publishes annually the NBA 2K companion app for mobile devices (the "App"), which allows users to initiate a process to create a customized player whose face resembles the user. *Id.* ¶¶ 12-13. To do this, the user opens the App, logs into his/her account, selects the "SCAN YOUR FACE" feature on the App, and takes 13 different pictures of his/her face using the mobile device's camera. *Id.* ¶ 13. The App then compresses and uploads the photographs to a Take 2 server. *Id.* ¶ 14. Next, the user logs into the gaming platform (e.g., X-Box), which is connected to the internet, and selects "Check for Head Scan Data" to build the custom player. *Id.* ¶¶ 97-100. With this selection, the user actually makes a request to AWS/Amazon servers, though there is no representation alerting the user of Defendants' involvement. *Id.* ¶ 105. At that point, Defendants retrieve the photographs and associated data from Take 2 and "construct a 3D face geometry of the user (the 'Face Geometry')" on their servers. *Id.* ¶ 106; *see also id.* ¶ 16. Defendants also obtain other information based on the Face Geometry used to identify the user. *Id.* ¶ 109. This all occurs behind the scenes—the video game screen only displays a circle filling in as it moves from 0% to 100% above the text: "Building your MyPLAYER's unique scanned head. This may take a few minutes." *Id.* ¶ 100.

Once they create the Face Geometry, Defendants transmit it, with information based thereon used to identify the user, through their various "regional" and "edge" server locations to deliver it to the user. *Id.* ¶¶ 107, 109. The Face Geometry constitutes a "biometric identifier" and the identifying information based thereon constitutes "biometric information" under BIPA (collectively referred to herein as "biometric data"). *Id.* ¶¶ 121-122. Defendants also store the biometric data at each original, regional, and edge server location through which it is transmitted. *Id.* ¶¶ 108, 110. The custom player is not stored on the gaming console's hard drive. Thus, the process of delivering and storing the biometric data through Defendants' various server locations is repeated each time the user plays with the previously-created custom player. *Id.* ¶¶ 114-117.

In 2021, D.M. took multiple photographs of his face with the App and logged onto his X-Box One in Illinois to create a custom NBA 2K player. *Id.* ¶ 134-137, 140, 144. Unbeknownst

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

to D.M., the request to create the custom player led Defendants to create, disseminate, and store his biometric data, including in and through Defendants' Illinois edge locations. *Id.* ¶¶ 141-152.

Defendants know they are collecting biometric data from Illinois citizens, including children, and Amazon has even hired a number of key executives from Take 2 including its co-founder and former president. *Id.* ¶¶ 126-131. Defendants have the ability to identify Illinois users and geo-fence unlawful conduct but choose not to. *Id.* ¶ 132. Moreover, Defendants profited from the biometric data services they provided, while repeatedly exposing D.M. and the Class to the risk of breach and invasion of privacy. *Id.* ¶¶ 74-76, 194, 221, 224, 227, 231, 241.

Nonetheless, Defendants have not developed, made publicly available, or complied with a written retention and destruction policy for such biometric data. *Id.* ¶¶ 171, 208. They have also improperly sold, traded, or profited from biometric data and disseminated it without consent from D.M. or his parent. *Id.* ¶¶ 137, 186-190, 197-198, 223-227, 234-235. Further, Defendants did not provide advance notice of their collection, capturing, receiving, or obtaining this biometric data, nor did they receive written releases before doing so. *Id.* ¶¶ 178-181, 215-218. Plaintiff seeks relief for Defendants' violations of BIPA § 15(a)-(d) and for unjust enrichment.

THE LEGAL STANDARD

"To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Miller v. Sawant*, 2021 U.S. App. LEXIS 33399, *9 (9th Cir. Nov. 10, 2021) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 677-78.

ARGUMENT

I. Plaintiff Plausibly Alleges Defendants Violated BIPA.

BIPA establishes standards of conduct for entities that possess or obtain biometric data. The Illinois legislature carefully crafted BIPA in 2008 to protect biometric data because "unlike other unique identifiers that are used to access finances or other sensitive information," biometric

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

identifiers cannot be changed; "[t]herefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." 740 ILCS 14/5(c).[1]

This case involves BIPA § 15(a)-(d). These subsections include an informed-consent regime requiring private entities to provide certain information and obtain written releases before they collect, capture, purchase, receive through trade, or otherwise obtain biometric data (§ 15(b)). Private entities in possession of biometric data must also develop a publicly available retention/destruction policy and comply with that policy (§ 15(a)); must not sell, lease, trade, or otherwise profit from a person's biometric data (§ 15(c)); and must not disclose, redisclose, or otherwise disseminate a person's biometric data without consent (§ 15(d)).

"[W]hen a private entity fails to comply with one of section 15's requirements, that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach." *Rosenbach v. Six Flags Entm't Corp.*, 129 N.E.3d 1197, 1206 (Ill. 2019); *see also Tims v. Black Horse Carriers, Inc.*, 2021 IL App (1st) 200563, ¶ 30. "Any person aggrieved by a violation" of BIPA can recover, *inter alia*, liquidated damages of $1,000 (if negligent) or $5,000 (if intentional or reckless) "for each violation." 740 ILCS 14/20. Finally, a plaintiff need not plead or prove additional consequences beyond the statutory violation. *Rosenbach*, 129 N.E.3d at 1206 ("No additional consequences need be pleaded or proved. The violation, in itself, is sufficient to support the individual's . . . statutory cause of action.").

A. Plaintiff States a Claim Under BIPA § 15(a).

Section 15(a) requires entities "in possession" of biometric data to develop a written retention and destruction policy, make that policy publicly available, and comply with the policy:

> A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention

[1] "Biometric identifiers" covered by BIPA include retina or iris scans, fingerprints, voiceprints, and scans of hand or face geometry. "Biometric information" includes "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." 740 ILCS 14/10.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

> schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

740 ILCS 14/15(a). Counts I and V plausibly allege that AWS and Amazon violated § 15(a) because they were in possession of Plaintiff's biometric data yet failed to develop, publish, and comply with a written retention/destruction policy.

1. Defendants are in possession of Plaintiff's biometric data.

Defendants argue they did not have to comply with § 15(a) because they were not "in possession" of biometric data. Def. Mot. at 5-8. BIPA does not define "possession." *See* 740 ILCS 14/10. The Illinois Supreme Court has defined "possession" as "'the act or condition of having in or taking into one's control or holding at one's disposal' and 'the fact of having or holding property in one's power; the exercise of dominion over property.'" *People v. Ward*, 830 N.E.2d 556, 560 (Ill. 2005) (quoting Webster's Third New Int'l Dictionary 1770 (1986); Black's Law Dictionary 1201 (8th ed. 2004)). Moreover, the ordinary meaning of "possession" does not contemplate exclusive control over property. *Id.* at 560-61; *see also Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 968 (N.D. Ill. 2020) ("*Heard I*") (holding "possession" in BIPA need not be "to the exclusion of others").

Here, Plaintiff plausibly alleges Defendants are in possession of biometric data. Defendants obtain photograph data from Take 2 servers and convert it into face geometry—a biometric identifier. Compl. ¶¶ 16, 106, 111. Once Defendants create the face geometry, they have it in their control. It remains in their control as they disseminate it and store it on their servers. *Id.* ¶¶ 107-117. Simply put, an entity that creates data, then disseminates and stores it, is in possession of that data.

Defendants argue they did not possess the biometric data because it was "exclusively owned" by Take 2, not Defendants. Def. Mot. at 7-8. This argument, however, relies on a factual premise outside the Complaint—Take 2's alleged ownership of the data. It also converts

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

BIPA's language from "possession" to "exclusive ownership." But "[o]wnership and possession are wholly distinct concepts." *United States v. Phillips*, No. 03 CR 465, 2005 U.S. Dist. LEXIS 1334, *5 (N.D. Ill. Jan. 10, 2005). For example, a thief, tenant, and vehicle lessee each possess property without owning it.

Defendants similarly argue that they don't possess the data because it was "exclusively . . . controlled by Take-Two." Def. Mot. at 8. This argument, too, presents a factual question, and one that requires Defendants to grossly misconstrue the Complaint. Although Defendants' physical storage of Plaintiff's biometric data sufficiently establishes possession, Plaintiff alleges Defendants took further actions that would be impossible absent control of the data: that Defendants—not Take 2—created the face geometry. *See, e.g.*, Compl. ¶ 16 ("AWS and/or Amazon then retrieves the face-scan data from the Take 2 server ***and converts it into a face geometry of the user*** on the AWS and/or Amazon servers, using AWS and/or Amazon computing power.") (emphasis added); *id.* ¶ 106 (Defendants "construct a 3D face geometry"); *id.* ¶ 111 (diagram with Step #4 stating: "Face Geometry Created by AWS/Amazon"). Defendants are, thus, more than a "third-party vendor with no relationship to D.M. whatsoever." Def. Mot. at 8; *see also Vance*, 525 F. Supp. 3d at 1312-13 (BIPA does not require entity to come into possession of biometric data directly from the person).

Even if Defendants had not created the biometric data, Plaintiff adequately alleges their possession of that data based on their dissemination and storage of it across their nationwide network. *See, e.g.*, Compl. ¶¶ 107-117. Defendants' heavy reliance on *Heard I* (Def. Mot. at 5-7), is misplaced as it ignores the same court's subsequent ruling denying the motion to dismiss the amended complaint. *See Heard v. Becton, Dickinson & Co.*, 524 F. Supp. 3d 831 (N.D. Ill. 2021) ("*Heard II*"). In *Heard I*, the plaintiff sued the manufacturer of a medication-dispensing device located in hospitals that required users to scan fingerprints. The court initially dismissed the complaint without prejudice because it "did not allege that [the defendant] 'exercised any form of control over the data or . . . held the data 'at [its] disposal.'" *Heard II*, 524 F. Supp. 3d at 840. The plaintiff then amended the complaint, adding allegations that the fingerprints were also

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

stored on the manufacturer's servers. *Id.* "Thus, the data was "not hermetically sealed within the hospital; users' biometric data flows back to [the manufacturer's] servers . . . ." *Id.* The plaintiff did not add allegations that the manufacturer could freely access the data, or that it exercised any control over the data, or even how the manufacturer received the data. *Id.* Still, the court found the complaint sufficient because it plausibly suggested the defendant "exercises some form of control over users' biometric data and therefore is in possession of the data." *Id.*

Similarly, Defendants here exercise some form of control over Plaintiff's biometric data. While the Court should not consider Defendants' extrinsic evidence outside the Complaint,[2] Defendants' reliance on portions of their websites to suggest that Take 2 has exclusive control over the data is misplaced. Def. Mot. at 7-8. The AWS Customer Agreement (Def. Mot. Ex. A) actually *evidences* Defendants' access to and control over the content in their servers. For instance, § 3.2 (quoted at Def. Mot. at 7), provides that AWS can and will access content to maintain or provide its services or to comply with laws. *Id.* (AWS "will not access or use Your Content ***except as necessary to*** maintain or provide the Service Offerings, or as necessary to comply with the law or a binding order of a governmental body.") (emphasis added)). Exhibit B to Defendants' Motion also states that AWS may disclose content to law enforcement, even without notice to the customer—further evidencing AWS' power and control over the data.[3]

As a practical matter, it is curious that Defendants argue they have no control over data they create, transmit, and store. Take 2 could lose the data if Defendants shut down their servers,

---

[2] In deciding whether to dismiss the complaint for failing to state a claim, the court is generally bound by the facts and allegations contained within the four corners of the complaint. *Hydrick v. Hunter*, 500 F.3d 978, 985 (9th Cir. 2007). The Complaint cites to four different websites hosted by Amazon, none of which are Defendants' Exhibits A-C. Defendants fail to meet the requirements to show that different webpages should be considered here. Defendants cannot show that "plaintiff's claim depends on the contents" of the four websites cited in footnotes of the Complaint. *Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005). Nor can they show that a viewer accessing the webpages cited by Plaintiff "must also access the surrounding pages" that Defendants have attached to their motion. *Id.*

[3] Exhibit C does not have any binding effect, as it: (a) "is for informational purposes only"; (b) "represents current AWS product offerings and practices, which are subject to change without notice"; (c) "does not create any commitments or assurances from AWS"; and (d) "is not part of, nor does it modify, any agreement between AWS and its customers." Def. Mot. Ex. C at ECF p. 52. Nonetheless, nothing in that document states that AWS customers retain exclusive ownership or control over content.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

if Defendants did not have adequate security measures and a breach occurred, or if someone physically walked into one of Defendants' data centers and took it—all because Defendants have it in their possession. AWS thus secures the data, stating it "has implemented sophisticated technical and physical measures against unauthorized access." Def. Mot. Ex. C at 4. To secure and prevent unauthorized access to property is to exert control and dominion over that property.

Furthermore, Defendants claim that that "[t]he mere transmission and storage of biometric data . . . is insufficient to state a claim absent any allegation of control over the data." Def. Mot. at 7. But BIPA expressly states it is meant to regulate, among other things, the "collection, use, safeguarding, handling, [and] storage" of biometric data. 740 ILCS 14/5(g). There are no qualifiers in the statute defining degrees of storage and transmission or suggesting that "mere" transmission or storage is insufficient. Defendants do not define a difference between "mere" storage and some other kind of storage, but simply assert that no Illinois court has imposed BIPA liability "on a company that . . . merely stores [biometric] data." Def. Mot. at 8. Yet just four days before Defendants filed their motion, a district court in Illinois found storage in a database as plausibly and "plainly" satisfying BIPA's "possession" requirement. *Naughton v. Amazon.com, Inc.*, No. 20-cv-6485, 2022 U.S. Dist. LEXIS 8, *9 (N.D. Ill. Jan. 3, 2022) ("[Plaintiff] also specifically asserts that Amazon stores his biometric data in a database. This plainly satisfies the 'possession' requirement at the pleadings stage.").

Nor do the two cases Defendants cite support their contention that "mere transmission and storage" is insufficient for possession under BIPA. Def. Mot. at 7 (citing *Heard I* and *Jacobs v. Hanwha Techwin Am., Inc.*, No. 21 C 866, 2021 U.S. Dist. LEXIS 139668 (N.D. Ill. July 27, 2021)). In *Jacobs*, like in *Heard I*, the court simply found inadequate allegations to proceed. *See* 2021 U.S. Dist. LEXIS 139668 at *9. In fact, the court in *Jacobs* pointed out cases finding plausible claims against technology providers where "the factual allegations made clear that the manufacturers of the fingerprint scanners had themselves collected, obtained, ***or stored*** the biometric data." *Id.* at *8 n.2 (citing *Figueroa v. Kronos*, 454 F. Supp. 3d 772 (N.D. Ill.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

2020); *Neals v. PAR Tech Corp.*, 419 F. Supp. 3d 1088 (N.D. Ill. 2019)) (emphasis added). Here, Defendants themselves created, transmitted, and stored the biometric data.

Finally, Defendants contend it would be absurd to apply § 15(a) to cloud computing services because it could require them to delete customer data. Def. Mot. at 8 n.5. But BIPA "obligates any private entity that collects a person's biometric information to comply with its requirements . . . . There is nothing absurd about that." *Neals*, 419 F. Supp. 3d at 1092; *see also Vance*, 525 F. Supp. 3d at 1313 (same) (citing *Neals*). Defendants' reliance on their factual assertions that they do "not create, control, or own the data" (Def. Mot. at 8 n.5), also contradicts Plaintiff's allegations as described above. Furthermore, removing data in compliance with the law would not violate any contractual terms with AWS's customers. In fact, the AWS Service Terms specifically allows AWS to remove customer data for a variety of reasons, including "in accordance with applicable law." AWS Service Terms,[4] ¶ 1.4 ("[W]e may remove or disable access to any Prohibited Content without prior notice . . . in accordance with applicable law . . . . In the event that we remove Your Content without prior notice, we will provide prompt notice to you unless prohibited by law."). These provisions allowing for the unilateral removal of data provide another plausible inference that Defendants had access to, control over, and held at their disposal—and therefore are in possession of—biometric data they create, disseminate, and store.

2. Plaintiff's § 15(a) claims are ripe.

"Ripeness is one of the justiciability doctrines that [courts] use to determine whether a case presents a live case or controversy." *Clark v. City of Seattle*, 899 F.3d 802, 808 (9th Cir. 2018). There are three obligations created by § 15(a). First, the entity in possession of biometric data must ***develop*** a written policy establishing a retention schedule and guidelines for permanently destroying biometric data. Second, the entity must make this written policy ***publicly available***. Third, the entity must ***comply*** with its established retention/destruction policy. Here, Plaintiff alleges Defendants violated § 15(a) by failing to ***develop*** a policy in the

[4] https://aws.amazon.com/service-terms/ (last visited Jan. 21, 2022). *See* Compl. ¶ 124. The service terms are also incorporated into the Customer Agreement attached to Defendants' Motion. *See* MTD Ex. A, ¶¶ 1.1, 14.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

first place and make it publicly available. Compl. ¶¶ 171-172. Because Defendants did not develop a policy in the first instance, they unlawfully retained Plaintiff's data by violating the first sentence of § 15(a). *See Kalb v. Gardaworld Cashlink LLC*, No. 1:21-cv-01092, 2021 U.S. Dist. LEXIS 81325, *7 (C.D. Ill. Apr. 28, 2021) (allegations of possession of biometric data without a written retention/ destruction policy "reasonably suggest[] Defendant has unlawfully retained this data"); *Wordlaw v. Enter. Leasing Co. of Chicago, LLC*, No. 20 CV 3200, 2020 U.S. Dist. LEXIS 239230, *10-11 (N.D. Ill. Dec. 21, 2020) ("[A]bsent a written policy or guidelines ensuring compliance, defendants' retention of plaintiff's fingerprint did not comport with BIPA.") (citations omitted); *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1274 (9th Cir. 2019) (affirming class certification where plaintiffs alleged a § 15(a) violation for Facebook's "failure to maintain a retention schedule or guidelines for destroying biometric identifiers").

As one district court recently explained, arguing that such claims are not ripe "doesn't make much sense" because the "failure to establish a retention and destruction policy involves a *current* violation, not a potential future one":

> [T]he fact that the [§15(a)] policy has to say something about destroying information no more than three years out doesn't suggest that the entity may wait those three years to establish its policy. The obligation under section 15(a) is, under the statutory language, a current obligation . . . . Thus a claim regarding its failure to establish a retention and destruction policy involves a *current* violation, not a potential future violation.

Nseumen v. Dal Glob. Servs., Inc., No. 21 C 2630, 2021 U.S. Dist. LEXIS 195566, *6 (N.D. Ill. Oct. 11, 2021). Moreover, because Defendants did not develop a policy, they *could not* have complied with it, thereby violating the second sentence of § 15(a). Thus, determining whether Defendants violated § 15(a) by failing to develop or comply with a written policy "present[s] issues that are definite and concrete, not hypothetical or abstract." *Clark*, 899 F.3d at 809.[5]

Section 15(a) also requires an entity that has not developed a written retention/ destruction policy to still permanently delete biometric data in the timeframe set by BIPA. This

[5] The Supreme Court has also "suggested, but did not decide, that once a court 'conclude[s] that [a plaintiff] ha[s] alleged a sufficient Article III injury,' any remaining prudential ripeness concerns do not render a plaintiff's claim nonjusticiable." *Clark*, 899 F.3d at 809 n.4 (quoting *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 167 (2014)). Here, Defendants have not raised any Article III challenges, nor could they. *See Patel*, 932 F.3d at 1274-75.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

duty, which is distinct from the duty to develop and comply with a written policy, is the requirement at the heart of Defendants' ripeness argument. Def. Mot. at 8-9. This was also the violation alleged in the two cases they cite. *See Bryant v. Compass Grp. USA, Inc.*, 503 F. Supp. 3d 597, 599 (N.D. Ill. 2020) (plaintiff alleged failure to delete data in timeframe required by § 15(a)); *Cothron v. White Castle Sys.*, 467 F. Supp. 3d 604, 612 (N.D. Ill. 2020) (same). Here, Defendants contend that adjudicating whether they violated this duty to delete data is not ripe because "the purpose for the alleged collection of Plaintiff's biometrics remains in effect." Def. Mot. at 9. Besides ignoring the other § 15(a) violations described above, this also misquotes BIPA, which requires deletion when the "initial" purpose for obtaining it "has been satisfied." 740 ILCS 14/15(a). The initial purpose was satisfied here when the data was delivered to D.M., and Defendants' possession of the data in multiple locations after the gameplay stops was not necessary to satisfy that initial delivery. Compl. ¶¶ 42-46, 58, 70. At the least, whether the initial purpose was satisfied is a factual question ripe for adjudication.

B. Plaintiff States a Claim Under BIPA § 15(b).

Section 15(b) states that a private entity may not "collect, capture, purchase, receive through trade, or otherwise obtain" a person's biometric data "unless it first": (1) informs the subject or the subject's legally authorized representative in writing (a) that biometric data is being collected or stored; and (b) of the specific purpose and length of term for which biometric data is being collected, stored, and used; and (2) receives a written release executed by the subject or legally authorized representative. 740 ILCS 14/15(b). Here, Defendants collected, captured, received through trade, or otherwise obtained D.M.'s biometric data when they created, disseminated, and stored that data, but they failed to first inform D.M. or his representative in writing and receive a written release. Thus, Counts II and VI allege plausible claims.

BIPA does not define "collect," "capture," "receive through trade," or "otherwise obtain," and "[i]t is entirely appropriate to employ the dictionary as a resource to ascertain the meaning of undefined terms." *Lacey v. Vill. of Palatine*, 904 N.E.2d 18, 26 (Ill. 2009) (quotations and citation omitted). The dictionary definition of "collect" includes "to gather" or

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

"to gain . . . control of." Merriam-Webster (Online ed. 2022).[6] The definition of "capture," also includes "gaining control." *Id.* "Control" means "to have power over." *Id.* Similarly, as Defendants acknowledge (Def. Mot. at 10), "obtain" means "to gain or attain usually by planned action or effort." Merriam-Webster (Online ed. 2022). The definitions of "gain" and "attain" include "to acquire or get possession of . . . ." and "to come into possession of." *Id.* Likewise, the definition of "receive" includes "to come into possession of." *Id.* Defendants argue these definitions require "some affirmative action by a private entity to acquire an individual's biometric information." Def. Mot. at 10. The definitions, however, do not inherently require affirmative action. If A deposits money into B's bank account, B has passively "come into possession of," "gain[ed] control of," and "has power over" that money.[7] Here, as discussed above, Defendants came into possession of or gained control of Plaintiff's biometric data when they created it, disseminated it, and/or stored it in their servers with the ability to access it, share access to it, and delete it. Thus, Defendants collected, captured, received, or obtained it.

Defendants also argue that the terms "possession" in § 15(a), (c), (d), and (e), must mean something different from the terms "collect, capture, . . . receive through trade, or otherwise obtain" found in § 15(b). *See* Def. Mot. at 10-11. The difference, they say, is that § 15(b) must involve some non-passive act beyond "mere possession." *Id.* at 10. Defendants point to inapposite cases to support this argument, including *Heard I*. *Id.*

Notably, Defendants overlook the statutory interpretation from *Figueroa*, decided less than two months after *Heard I*, which rejected the same arguments made by Defendant here. There, the court explained that the sections of BIPA such as § 15(a), which use the term "in possession," placed duties on entities that already possessed biometric information before BIPA's effective date, while § 15(b) placed duties on entities coming into such possession (that

[6] Merriam-Webster (Online ed. 2022) is available at https://www.merriam-webster.com/dictionary/.

[7] Another example is property mailed to someone else's residence. Defendants note that "obtain" means "to gain or attain usually by planned action or effort." Def. Mot. at 10. But "usually" means planned action or effort is not necessarily needed, as shown by these examples.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

is, entities that "may . . . obtain" the data) after BIPA's effective date. *Figueroa*, 454 F. Supp. 3d at 784 (citing various sections of the statute). That distinction mattered:

> Section 15(a) imposes different obligations than Section 15(b)—Section 15(a) requires entities to develop and publish written policies regardless of whether they obtained biometric data before or after BIPA's effective date, while Section 15(b) sensibly imposes notice and consent obligations only on those entities that come into possession of such data after BIPA's effective date. Interpreting the term "obtain" in Section 15(b) to include Kronos's conduct therefore does not render Section 15(a) superfluous.

Id. In fact, in *Heard II*, the court adopted *Figueroa*'s reasoning. *See Heard II*, 524 F. Supp. 3d at 841 ("As another district court has explained, however, Section 15(b) applies prospectively to the collection of biometric data after the date of BIPA's enactment, while other sections of the Act are aimed at defendants who had collected data before BIPA was adopted and remained in possession of that data.") (citing *Figueroa*, 454 F. Supp. 3d at 783-84); *see also id.* at 841-43 ("The court agrees with the *Figueroa* court's interpretation of the statute . . . .").

Accordingly, *Heard II* found the plaintiff stated a § 15(b) claim by alleging the defendant came into possession of fingerprints after BIPA's enactment. *Id.* at 841 ("The fingerprint scans at issue in this case were collected after the enactment of BIPA, and [defendant] is in possession of that data because it remains stored on [defendant's] servers, so it is fair to conclude that [defendant] collected or otherwise obtained the data for purposes of Section 15(b)."). Whether the defendant took an "active step" was no longer determinative to the court.[8]

Finally, even if some active step was required, the details regarding Defendants' collection of biometric data from photographs and dissemination of that data across its network sufficiently alleges additional active steps by Defendants to collect, capture and obtain Plaintiff's biometric data. Compl. ¶¶ 16, 97-102, 106, 111. Defendants' assertions that Take 2, not AWS,

[8] The other cases Defendants rely on to argue an "affirmative action" is required (Def. Mot. at 10) involved a different context—a third party that simply supplied the technology used by a different entity to collect biometric data (each with insufficient allegations). *See Jacobs*, 2021 U.S. Dist. LEXIS 139668 at *9 (no allegations seller of security cameras received biometric data); *Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 286 (N.D. Ill. 2019) (technology used to collect fingerprints provided by defendant); *Bernal v. ADP, LLC*, No. 2017-CH-12364 (Cir. Ct. Cook Cnty., Aug. 23, 2019) (defendant supplied plaintiff's employer with the technology); *see also Vance*, 525 F. Supp. 3d at 1314 ("[T]hese cases concern complaints that do not sufficiently plead the role of the third-party, thus warranting dismissal.").

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

creates biometric data is either a misstatement or misunderstanding of Plaintiff's allegations.[9] Even if Plaintiff had not provided such detail concerning Defendants' actions, the existence of the subject biometric data on their servers is sufficient evidence they "obtained" it for the purposes of § 15(b), as it was in *Heard II*. *See also Vance*, 525 F. Supp. 3d at 1313 ("Indeed, Amazon does not explain how it could have come into possession of or used Plaintiffs' facial scans without having first obtained it."); *Figueroa*, 454 F. Supp. 3d at 784 ("[T]o have [stored or used] the data, [the defendant] necessarily first had to 'obtain' the data."). Defendants' creation of a face geometry that previously did not exist and/or their dissemination and storage of it constitute affirmative actions in the collection, capture, receipt, or obtaining of biometric data. Defendants thus violated § 15(b) by failing to first comply with its informed-consent regime.

C. Plaintiff States a Claim Under BIPA § 15(c).

Section 15(c) states that "[n]o private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information." 740 ILCS 14/15(c). "[T]hese terms contemplate a transaction in which an item is given or shared in exchange for something of value." *Vance*, 534 F. Supp. 3d at 1321. "Thus, § 15(c) regulates transactions with two components: (1) access to biometric data is shared or given to another; and (2) in return for that access, the entity receives something of value." *Id.* at 1322.

Here, Defendants received money to create, disseminate, and store the biometric data of Plaintiff and the putative Class. Compl. ¶¶ 83-84, 104-122, 187-188; *see also Flores v. Motorola Sols., Inc.*, No. 1:20-cv-01128, 2021 U.S. Dist. LEXIS 21937, *8 (N.D. Ill. Jan. 8, 2021) (§ 15(c) claim stated where defendants allegedly extracted and stored biometric identifiers and offered access to the stored data for a fee). Equally, the biometric data was shared between

[9] Defendants point to Plaintiff's allegations that the photograph data collected from the App "is compressed and uploaded to a Take 2 server" to suggest Take 2 created the data. Def. Mot. at 11. But "compress" simply means the photograph is reduced to a smaller size. *See* Merriam-Webster (Online ed. 2022). There are no allegations that Take 2 makes the biometric data. Instead, the App uploads the photographs, and Defendants create the biometric data using the compressed photographs. Compl. ¶¶ 97, 106.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Defendants and Take 2 in exchange for money. The Customer Agreement attached to Defendants' Motion provides that Take 2's "right to access or use" the data in Defendants' possession will be suspended if it breaches its payment obligation. Def. Mot. Ex. A § 6.1(c); *see also id.* § 7.3(b)(ii) (upon termination of the agreement (not for cause), Defendants will only allow customer to access and retrieve data if payment has been made in full). In other words, Defendants share, and allow Take 2 to access, the biometric data for a fee. If payment stops, Take 2's access stops.[10] Thus, Defendants violated § 15(c) because they shared or gave access to biometric data in exchange for something of value. Furthermore, Defendants profited from marketing, selling, and performing biometric data storage and delivery services that included creating, collecting, and transmitting biometric data of D.M. and the Class. Compl. ¶¶ 190, 227.

Defendants attack the § 15(c) claim by again disputing that they were paid to create the biometric data. *See* Def. Mot. at 12 (citing Compl. ¶¶ 93-103). This factual challenge requires a gross misreading of the Complaint. Paragraphs 93-103 say nothing about Take 2 creating biometric data—much less make such allegations "explicitly and in detail." Def. Mot. at 13. Instead, paragraphs 93-96 describe a user's experience of photographing his/her face into the NBA 2K App. The photographs are sent to the Take 2/2K Games' servers. Compl. ¶ 97. Paragraphs 98-103 describe what the user sees on his/her screen when creating a custom player.

Defendants ignore the next 18 paragraphs of the Complaint, which are placed under the heading "Behind the Scenes, AWS/Amazon Obtains, Possesses, Transmits, and Stores Biometric Identifiers and/or Biometric Information from Users of the NBA 2K Games and Apps." Compl. ¶¶ 104-122. As the title suggests, these paragraphs describe what is actually happening "behind the scenes" that the user does not see on the screen. Paragraphs 105-106 provide detailed allegations that Defendants retrieve the photographs and associated data from the Take 2 servers and create the face geometry that is the biometric identifier at issue in the case. *See* Compl. ¶ 106 (Defendants "construct a 3D face geometry of the user"); *id.* ¶¶ 16, 111.

[10] It is unclear what Defendants will do with D.M.'s biometric data if Take 2 never pays or its Agreement is terminated for cause.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Defendants are also wrong that these allegations contradict other portions of the Complaint describing cloud-computing services. Def. Mot. at 12-13. Defendants again misconstrue and ignore the actual allegations, which repeatedly include "computing power" as one of the many technology services provided by Defendants. *See, e.g.*, Compl. ¶ 84 ("Take 2 and/or 2K Games use AWS/Amazon cloud-computing for, *inter alia*, servers, ***computing***, storage, and to provide the infrastructure . . . ."); *id.* ¶¶ 39, 41, 65. The biometric data is created "on the AWS and/or Amazon servers, using AWS and/or Amazon computing power." Compl. ¶ 16; *id.* ¶ 106 (same). Thus, the allegations that Defendants created the biometric data are consistent with the description of services Defendants provide.

Finally, Defendants argue that Plaintiff must allege a direct sale of biometric data. Def. Mot. at 13 (citing *Vance*, 534 F. Supp. 3d at 1307). But BIPA's plain language does not require a direct, exclusive, or itemized sale of biometric data. Nor does *Vance* require it. In *Vance*, this Court explained that a direct sale is one example of the first component of a regulated transaction (when access to biometric data is shared or given to another). *Vance*, 534 F. Supp. 3d at 1322. But the Court did not say that only a direct sale satisfies this component. In fact, the Court described § 15(c) as simply "prohibiting for-profit transactions involving biometric data . . . to control the spread of biometric data." *Id.* at 1323 n.4. Here, the transaction involves "the commercial dissemination of biometric data for some sort of gain . . . ." *Id.* 1322. Thus, Defendants sold, leased, traded, or profited from biometric data in violation of § 15(c).

D. Plaintiff States a Claim Under BIPA § 15(d).

Section 15(d) provides that a private entity "in possession" of biometric data may not "disclose, redisclose, or otherwise disseminate" a person's biometric data without the consent of the subject of biometric data or his/her authorized legal representative. 740 ILCS 14/15(d). Counts IV and VIII plausibly allege that AWS and Amazon, respectively, violated BIPA § 15(d) because they disseminated and/or disclosed Plaintiff's biometric data without consent.

Defendants wrongly contend § 15(d) claims must involve disclosures to third-parties. Def. Mot. at 14. The text of § 15(d) does not contain a third-party requirement, nor is it limited

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

to disclosures. It also prohibits dissemination of biometric data. "Disseminate" means "to spread abroad as though sowing seed" or "to disperse throughout." Merriam-Webster (Online ed. 2022).[11] Here, Plaintiff alleges Defendants disseminated his biometric data every time they moved it to, and stored it in, a different server in a different location across the nation. *See, e.g.*, Compl. ¶ 111, Fig. 4; ¶¶ 55-56, Fig. 1-3; ¶¶ 71-73, 105-111, 115-117, 197, 234. By spreading it to multiple locations, Defendants put Plaintiff's data at risk of breach, interception, or loss.

The cases Defendants cite do not "uniformly recognize" a third-party requirement. Def. Mot. at 14. These cases discuss third-party disclosures in the context of what the plaintiff alleged. *See Roberson v. Maestro Consulting Sers. LLC*, 507 F. Supp. 3d 998, 1010 (S.D. Ill. 2020) (using the term "third parties" only one time—in a quote from the complaint in the *Cothron* case); *Heard II*, 524 F. Supp. 3d at 843 (describing allegations of disclosure to third parties); *Bradenberg v. Meridian Senior Living, LLC*, No. 20-cv-03198, 2021 U.S. Dist. LEXIS 188305, *2 (C.D. Ill. Sep. 30, 2021) (same); *Namuwonge*, 418 F. Supp. 3d at 285 (plaintiff attempted to plead disclosure to third party). While these cases suggest a third-party disclosure falls under § 15(d), none of them hold that § 15(d) is *limited* to disclosures to third parties, and none concerned the nationwide dissemination of the plaintiff's face geometry.

Even though § 15(d) does not require a third-party disclosure, Plaintiff adequately alleges such disclosure here. In *Roberson*, the court held the plaintiff had standing to pursue a § 15(d) claim based on allegations that the defendant "'disclosed, redisclosed, or disseminated the biometric information of plaintiffs and the class members to, through, and/or among others, including but not limited to ***other [Defendants'] entities*** or persons associated with [Defendants]." 507 F. Supp. 3d at 1010 (emphasis added); *see also Naughton*, 2022 U.S. Dist. LEXIS at *9-10 ("Amazon seeks to impose a heightened standard where there is none; all Naughton must plead is 'plausible dissemination.' He has done so here by indicating that Amazon has collected his facial geometry, disclosed that data ***to 'other Amazon entities'*** and to

[11] "Abroad" in the first definition means "over a wide area: widely." *See id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

'third-party biometric device and software vendor(s)' and other possible third parties.") (citing *Cothron*, 467 F. Supp. 3d at 618) (emphasis added) (additional citations omitted).

Similarly, here Plaintiff alleges disclosure of biometric data "to, through, and/or among others," including the related entities of AWS and Amazon. For instance, Plaintiff alleges that AWS and Amazon have "shared facilities" and a "shared infrastructure," which includes data centers used by AWS that Amazon owns and operates, CloudFront IP addresses utilized by AWS that Amazon owns, and servers, networks, and other equipment owned by Amazon. Compl. ¶¶ 59-63. As alleged, each time the biometric data passes through and is stored in a new location, it is disclosed or disseminated to other entities—that is, to, through, or among AWS and Amazon. Additionally, Defendants share access to the biometric data with Take 2. *See* § I.C, *supra*; s*ee also* Def. Mot. at 7-8 (describing how Defendants allow Take 2 to access the biometric data). Thus, as in *Roberson* and *Naughton*, Plaintiff has alleged plausible dissemination by indicating that Defendants created and stored his facial geometry, and disclosed that data to or through other Amazon entities and to other third parties. "The law does not demand more at the pleadings stage." *Naughton*, 2022 U.S. Dist. LEXIS 8 at *10.

Finally, the Complaint does not "necessarily concede" that Plaintiff consented to the dissemination. Def. Mot. at 15. First, the Complaint alleges that Plaintiff neither knew of nor consented to Defendants' dissemination of biometric data. Compl. ¶¶ 198, 235. These allegations must be taken as true. Second, D.M. is a minor, and BIPA requires the consent of D.M.'s "legally authorized representative," which was never received. 740 ILCS 14/15(d)(1). Third, Plaintiff does not allege that he knew AWS or Amazon was ever involved in the process. Instead, Plaintiff alleges that when playing the game online, "it appears as though the gaming platform is transmitting images to the user's television." Compl. ¶ 71; *see also id.* ¶¶ 104-122 (describing what occurs "behind the scenes"). Without any disclosure of the behind-the-scenes process, there could be no "informed consent." *See Roberson*, 507 F. Supp. 3d at 1009 (§ 15(d) is part of BIPA's "'informed-consent regime'") (quoting *Cothron*, 467 F. Supp. 3d at 613).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

II. Plaintiff Plausibly Alleges A Claim for Unjust Enrichment.

Defendants argue Washington law applies to Plaintiff's unjust enrichment claim. This is at odds with this Court's findings in *Vance*, a case that involved claims of BIPA violations and unjust enrichment. There "[t]he court concluded that under step one of Washington's two-step approach to choice-of-law questions, an actual conflict between Washington and Illinois law exists over whether Plaintiffs must plead that they suffered an economic expense distinct from a privacy harm." *Vance*, 534 F. Supp. 3d at 1324. The Court then conducted Washington's two-step "most significant relationship" test and found Illinois law should apply. *Id.* at 1324-27.

The same result is warranted here. "First, the court considers the states' relevant contacts to the cause of action. Second, if those contacts are evenly balanced, the court considers the interests and public policies of [the two] states and . . . the manner and extent of such policies as they relate to the transaction in issue." *Id.* at 1324-25 (citation and quotation marks omitted). "'In actions for restitution, the rights and liabilities of the parties with respect to the particular issue are determined by the local law of the state which, with respect to that issue, has the most significant relationship to the occurrence and the parties under the principles stated in § 6.'" *Id.* at 1325 (quoting Restatement (Second) of Law on Conflict of Laws ("Restatement") § 221(1)). In applying these principles, courts consider the contacts set forth in Restatement § 221(2). *Id.* "The court's approach is not merely to count contacts but rather to consider which contacts are the most significant and where those contacts are found." *Id.* (citation omitted).

Here, the contacts weigh in favor of Illinois. The first contact the court examines is "[t]he place where a relationship between the parties was centered, provided that the receipt of enrichment was substantially related to the relationship." Restatement § 221(2)(a). To the extent the relationship between D.M. and Defendants was centered in one location, it was Illinois. That is where D.M. unknowingly contacted and interacted with Defendants. Compl. ¶ 134-144. It is also where D.M.'s biometric data was stored and disseminated. *See, e.g.*, *id.* ¶ 152. Still, D.M. did not contract with Defendants, so this factor should be given little, if any, weight. *Vance*, 534

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

F. Supp. 3d at 1326 (citing *Veridian Credit Union v. Eddie Bauer, LLC*, 295 F. Supp. 3d 1140, 1154 (W.D. Wash. 2017) (factor bears "little, if any, weight" when parties did not contract).[12]

The second contact is "[t]he place where the benefit or enrichment was received." Restatement § 221(2)(b). Here, as in *Vance*, "the core of the benefit lies in Plaintiffs providing images of their faces." *Id.* at 1326. Defendants offer no argument on where this benefit was received, but "Amazon's nation-wide reach, as alleged, supports the inference that the place where the benefit was received may span many states." *Id.*; *see also* Compl. ¶¶ 40-41, 48-57, 59-64. Ultimately, this factor is neutral. *See Vance*, 534 F. Supp. 3d at 1326 (citing Restatement § 221(2) cmt. d) (assigning factor "little or no weight" when place where benefit was received "bears little relation to the occurrence . . . or where this place cannot be identified").

The third contact is "[t]he place where the act conferring the benefit or enrichment was done." Restatement § 221(2)(c). Plaintiff conferred the benefit in Illinois. Compl. ¶¶ 154-155. D.M. "and all putative class members are Illinois residents who uploaded Illinois-created content in Illinois." *Vance*, 534 F. Supp. 3d at 1326. "Although there are other acts in the chain of events leading to Amazon benefiting off of Plaintiffs' biometric data, including actions Amazon allegedly took itself, the core of the benefit lies in Plaintiffs providing images of their faces" for which Defendants received benefits. *Id.*; *see also supra*, § I.C; Compl. ¶ 241. "Thus, this factor, which is assigned particular weight given the neutrality of the place where the benefit was received, counsels application of Illinois law." *Vance*, 534 F. Supp. 3d at 1326.

The fourth contact is "[t]he domicile, residence, nationality, place of incorporation and place of business of the parties." Restatement § 221(2)(d). Here, despite the different domiciles of the parties (Illinois, Delaware, Washington), the contacts are grouped in Illinois, where Defendants do business. "Plaintiffs are domiciled there, the benefiting act (the sharing of facial images) was done there, and Amazon . . . conducts business there related to the enrichment at

[12] *See also id.* at 1326 n.6 ("[T]he unjustness stems from the lack of consent from Plaintiffs in Illinois. Thus, it is unclear whether this first factor . . . would ever be applicable in cases such as these.").

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

issue." *Vance*, 534 F. Supp. 3d at 1327; Compl. ¶¶ 51-52, 56, 64, 73, 118-120, 151-153. This factor "tip[s] towards Illinois." *Vance*, 534 F. Supp. 3d at 1327.

The last contact is "[t]he place where a physical thing, such as land or a chattel, which was substantially related to the enrichment, was situated at the time of the enrichment." Restatement § 221(2)(e). This factor is neutral here because "[the] allegations revolve around the benefits obtained from intangible notions of biometric data." *Vance*, 534 F. Supp. 3d at 1326.

Accordingly, Illinois has the most significant relationship to this occurrence. The Restatement also "recognizes that [predictability and uniformity of result] are furthered by choosing the state where the invasion of privacy occurred, as that location will usually be readily ascertainable. . . . That is especially true here, as this court and others have opined on the difficulty of pinpointing where events occurred in BIPA cases." *Id.* at 1327-28 (citations omitted). Here, Defendants' conduct violated privacy rights, the "harm occurred in Illinois and is ongoing," and "the required BIPA disclosures and permissions would have been obtained and executed in Illinois." Compl. ¶ 153. Finally, "even if the contacts were balanced, Illinois has the greater interest in determining this particular issue" because "[a]pplication of its unjust enrichment law, which recognizes privacy harms, aligns with and strengthens Illinois's general regulatory scheme regarding privacy interests." *Vance*, 534 F. Supp. 3d at 1328, 1329.

Thus, Illinois law applies to Plaintiff's unjust enrichment claim. "[U]nder Illinois law, 'the assertion that plaintiffs are 'exposed to a heightened risk of privacy harm' and 'have been deprived of their control over their biometric data' sufficiently states an unjust enrichment claim.'" *Id.* at 1328 (quoting *Vance v. IBM*, No. 20 C 577, 2020 U.S. Dist. LEXIS 168610, *12-14 (N.D. Ill. Sep. 15, 2020)). Here, Plaintiff alleges Defendants profited off of Plaintiff and the Class' biometric data, while "exposing Plaintiff and Class Members to a heightened risk of privacy and informational harms and depriving them of their control over their biometric data." Compl. ¶ 241. "Because Plaintiffs have so pleaded, they have sufficiently stated a claim for unjust enrichment under Illinois law." *Vance*, 534 F. Supp. 3d at 1328.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Finally, as Defendants recognize, under Illinois law, an unjust enrichment claim based on improper conduct alleged in another claim "stands or falls with the other claim." Def. Mot. at 16 (citing cases). Thus, the unjust enrichment claim survives with the BIPA claims.[13]

III. Plaintiff Adequately Alleges Claims Against Defendant Amazon.Com, Inc.

Rule 8(a)(2) requires "only a short and plain statement of the claim showing that the pleader is entitled to relief, in order to give the defendant fair notice of what the . . . claim is and the grounds upon which it rests." *Twombly*, 550 U.S. at 555 (citations and quotation marks omitted). Amazon argues it is "impossible to tell" what claims are asserted against it based on allegations grouping Defendants together. Def. Mot. at 19. But "[g]roup pleading is not fatal to a complaint if the complaint still gives defendants fair notice of the claims against them." *In re Pac. Fertility Cent. Litig.*, No. 18-cv-01586-JSC, 2019 U.S. Dist. LEXIS 133922, *10 (N.D. Cal. Aug. 8, 2019) (citation omitted). "For example, where the defendants are alleged to be 'related entities' who acted in concert 'it is entirely possible that the allegations of wrongdoing are intended to include each and every entity defendant.'" *Id.* at 11-12 (quoting *Tivoli LLC v. Sank*ey, No. SA CV 14-1285-DOC (JCGx), 2015 U.S. Dist. LEXIS 189660, *11 (C.D. Cal. Feb. 3, 2015); citing *Munning v. Gap, Inc.*, No. 16-CV-03804-TEH, 2016 U.S. Dist. LEXIS 149886, *9 (N.D. Cal. Oct. 28, 2016) ("[B]ecause the Defendants all share a parent-subsidiary relationship . . . and because all the Defendants are represented by the same counsel, frustration of notice of the claims to each defendant is unlikely.")).

Moreover, the *Adobe* case relied on by Amazon actually supports Plaintiff. There, the allegations "that all the Defendants infringed on Adobe's trademarks and copyrights, and that Blue Source specifically sold infringing products . . . . provide[d] sufficient notice to [Blue Source] as to the nature of the claims asserted, including what conduct is at issue." *Adobe Sys. v. Blue Source Grp. Inc.*, 125 F. Supp. 3d 945, 965 (N.D. Cal. 2015) (citations and quotation marks omitted). In addition, the separate causes of action against specified defendants "sufficiently

[13] *See, e.g.*, *Vance*, 534 F. Supp. 3d at 1328 n.7; *In re Clearview AI, Inc.*, No. 21-cv-135, 2022 U.S. Dist. LEXIS 14882, *19 (N.D. Ill. Jan. 27, 2022); *In re Flores*, 2021 U.S. Dist. LEXIS 21937 at *9.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

put[] Blue Source on notice as to which causes of action apply to Blue Source." *Id.* (citing *Vasquez v. Bank of Am., N.A.*, 2013 U.S. Dist. LEXIS 161244, *15 (N.D. Cal. Nov. 12, 2013) (Rule 8 satisfied where plaintiff specified which defendants were subject to the separate causes of action)); *see also In re Pac. Fertility*, 2019 U.S. Dist. LEXIS 133922, at *11-12 ("While the background allegations often include 'and/or' language with respect to [two defendants], the allegations under each of the claims are as to each defendant separately. . . . Further, given the close relationship between these defendants and the fact that they share the same counsel, they are aware of the actions they may have taken to give rise to Plaintiffs' legal claims.").[14]

Here, as discussed in § I.D above, Plaintiff alleges integration of AWS and Amazon services. Compl. ¶¶ 59-64. While AWS enters contractual relationships with video game companies (Compl. ¶¶ 65, 67-68), AWS utilizes Amazon's "shared facilities" and "shared infrastructure" to provide such services (*id.* ¶¶ 66, 61-63, 9, 11). The integration of AWS and Amazon as alleged supports a plausible inference that each has possession and control over the data in their shared infrastructure. Moreover, Plaintiff alleges that each Defendant created, possessed, obtained, profited off of, and disseminated biometric data, as evidenced by the separate counts against them. Thus, Amazon, who is represented by the same counsel as AWS, has sufficient notice of D.M.'s claim that Amazon was in possession of D.M.'s biometric data and violated § 15(a) (c), and (d) (Counts V, VII, VIII); that Amazon obtained D.M.'s biometric data in violation of § 15(b) (Count VI); and that Amazon was unjustly enriched (Count IX).

CONCLUSION

For the reasons set forth above, Defendants' Motion to Dismiss should be denied.

[14] Defendants' reliance on *Destfino v. Reiswig*, 630 F.3d 952 (9th Cir. 2011) is misplaced as that case affirmed dismissal of allegations against multiple defendants in a fraud claim under the heightened pleading requirements of Rule 9(b). *See id.* at 958.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

DATED this 16th day of February, 2022.

TOUSLEY BRAIN STEPHENS PLLC

By: *s/ Jason T. Dennett*
s/ Cecily C. Jordan

Jason T. Dennett, WSBA #30686
Cecily C. Jordan, WSBA #50061
jdennett@tousley.com
cjordan@tousley.com
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
Telephone: 206.682.5600
Fax: 206.682.2992

Kevin P. Green
kevin@ghalaw.com
GOLDENBERG HELLER & ANTOGNOLI, P.C.
2227 South State Route 157
Edwardsville, IL 62025
Telephone: 618-656-5150
Facsimile: 618-656-6230

Christian G. Montroy
montroy@montroylaw.com
MONTROY LAW OFFICES LLC
2416 North Center
PO Box 369
Maryville, IL 62062
Telephone:618-223-8200

Attorneys for Plaintiff and the Proposed Class